COMMITTEE ON GOVERNMENT REFORM

TOM DAVIS, CHAIRMAN

MEDIA ADVISORY

For Immediate Release
March 14, 2006

Contact: Robert White / Drew Crockett
(202) 225-5074

Is the Government Ready for a Digital Pearl Harbor?

Davis to Unveil 2005 Federal Computer Security Report Cards

Do We Still Have D+ Computer Systems?

What: **Government Reform Committee Oversight Hearing: "No Computer System Left Behind: A Review of the 2005 Federal Computer Security Scorecards"**

When: **THURSDAY, MARCH 16, 2006, 10:00 A.M.**

Where: **ROOM 2154, RAYBURN HOUSE OFFICE BUILDING**

Background:

Our economy and government have become more and more dependent on information technology and the Internet. Government agencies have improved the efficiency of their operations and services to citizens through electronic government initiatives. Given the interconnectivity of systems, all it takes is one weak link to break the chain.

We must guard our information systems from hackers, terrorists, hostile foreign governments, and identity thieves to protect our national security, allow for continuity of government operations, and ensure the privacy of citizens' personal information.

An attack could originate anywhere at anytime. Unfortunately, last year's overall grade for the government was only a D+.

One of the best ways to defend against attacks is to have a strong, yet flexible, protection policy in place. Chairman Tom Davis wrote the Federal Information Security Management Act of 2002 (FISMA) to accomplish this by requiring each agency to create a comprehensive riskbased approach to agency-wide information security management. Therefore, compliance with the Act is critical to protect our economy and national security.

The FISMA reports submitted to Congress by the agency Chief Information Officers (CIOs) and the Inspectors General (IGs) are used to compile the Committee's annual scorecards, which help us gauge government information security progress. The Committee will review the results of the agencies' 2005 FISMA reports, identify strengths and weaknesses in government information security, and explore reasons for continued unacceptable performance by some agencies. Overall, the Committee will evaluate whether federal computer operations are prepared for a major cyber-attack.

Witnesses:

Panel One

Gregory C. Wilshusen, Director, Information Security Issues, Government Accountability Office
Karen S. Evans, Administrator, Office of E-Government and Information Technology, Office of Management and Budget

Panel Two

Patrick Pizzella, Assistance Secretary for Administration and Management, Department of Labor
Tom Hughes, Chief Information Officer, Social Security Administration
Robert F. Lentz, Director of Information Assurance, Department of Defense
Scott Charbo, Chief Information Officer, Department of Homeland Security

###